2. PERMUTATION GROUPS

Definition 52 *Let S be a set. A bijection $S \to S$ is called a* ***permutation*** *of S and the set of permutations of S is denoted* $\mathrm{Sym}(S)$.

If n is a positive integer, then we write S_n for $\mathrm{Sym}\left(\{1, 2, \ldots n\}\right)$.

Notation 53 ***Important:*** *though this convention is not universal, in Oxford it is usual to write permutations on the right. So for $k \in \{1, 2, \ldots, n\}$ and $\sigma, \tau \in S_n$ then we would write $k\sigma$ for $\sigma(k)$ and $k\sigma\tau$ for $\tau(\sigma(k))$. So the permutation $\sigma\tau$ is the composition of σ first with τ second.*

Theorem 54 *Let S be a set.*
(a) Then $\mathrm{Sym}(S)$ *forms a group under composition. It is called the* ***symmetry group*** *of S.*
(b) If $|S| \geqslant 3$ then $\mathrm{Sym}(S)$ *is non-abelian.*
(c) The cardinality of S_n is $n!$

Proof. (a) We know that the composition of two bijections is a bijection. So $\circ$ is indeed a binary operation on $\mathrm{Sym}(S)$. Further for any $f, g, h \in \mathrm{Sym}(S)$ and $x \in S$ we have

$$x\left((fg)\,h\right) = \left(x\,(fg)\right)h = \left((xf)\,g\right)h = (xf)\,(gh) = x\,(f\,(gh))$$

So $\circ$ is an associative binary operation. The identity of $\mathrm{Sym}(S)$ is easily seen to be the identity map

$$id_S(x) = x \qquad \text{for all } x \in S$$

and the inverse of $f \in \mathrm{Sym}(S)$ is, unsurprisingly, its inverse map f^{-1}.

(b) If x_1, x_2, x_3 are three distinct elements of S then we can define two permutations of S by

$$\begin{aligned} f &: x_1 \mapsto x_1, \quad x_2 \mapsto x_3, \quad x_3 \mapsto x_2, \quad x \mapsto x \text{ for other } x; \\ g &: x_1 \mapsto x_2, \quad x_2 \mapsto x_1, \quad x_3 \mapsto x_3, \quad x \mapsto x \text{ for other } x; \end{aligned}$$

which do not commute as

$$\begin{aligned} fg &: x_1 \mapsto x_2, \quad x_2 \mapsto x_3, \quad x_3 \mapsto x_1, \quad x \mapsto x \text{ for other } x. \\ gf &: x_1 \mapsto x_3, \quad x_2 \mapsto x_1, \quad x_3 \mapsto x_2, \quad x \mapsto x \text{ for other } x; \end{aligned}$$

(c) For $f \in S_n$ there are n possibilities for $1f$, but as f is 1-1, and so $1f \neq 2f$, there are $n-1$ possibilities for $2f$ once $1f$ is known and likewise $n-2$ possibilities for $3f$ etc. In all then there are

$$n \times (n-1) \times (n-2) \times \cdots \times 1 = n!$$

permutations of $\{1, 2, \ldots, n\}$. ■

One (slightly cumbersome) way of writing down a permutation $\sigma \in S_n$ is as an array

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1\sigma & 2\sigma & 3\sigma & \cdots & n\sigma \end{pmatrix}$$

though we shall improve on this notation with the introduction of *cycle notation.*

Example 55 *(i) So S_2 is a group of order two which contains the elements*

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

The first element is the identity and the second is self-inverse.

(ii) And S_3 is a group of order six with contains the elements

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

The first element is e. If we write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

then we see (amongst other things) that

$$\begin{aligned}
\sigma^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \\
\sigma^3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e; \\
\tau^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = e; \\
\sigma\tau &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; \\
\tau\sigma^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.
\end{aligned}$$

The six elements of S_3 are in fact

$$e, \qquad \sigma, \qquad \sigma^2, \qquad \tau, \qquad \sigma\tau, \qquad \sigma^2\tau.$$

The Cayley table for S_3 is

$*$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

Remark 56 *Note that the six permutations listed above as the elements of S_3 are the same as those listed in Example 35 and the above Cayley table for S_3 is identical to that in Example 41 once σ, τ are replaced with r, s. This shows that D_6 and S_3 are in fact isomorphic.*

Example 57 *Set*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \qquad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix},$$

in S_5. Determine the product $\alpha\beta\gamma$, the inverse of β and the order of γ.

Solution. We have

$$\begin{aligned}
\alpha\beta\gamma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}; \\
\beta^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 4 & 5 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}; \\
\gamma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}, \qquad \gamma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}, \qquad \gamma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}, \\
\gamma^5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}, \qquad \gamma^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e,
\end{aligned}$$

so that the order of γ is 6. ■

There is a special type of permutation, a *cycle*, which shall prove useful as we shall see that any permutation can be (essentially) uniquely decomposed as a product of cycles.

Definition 58 *A permutation $\sigma \in S_n$ is a **cycle** if there are distinct elements $a_1, a_2, \ldots, a_k$ in $\{1, 2, \ldots, n\}$ such that*

$$a_i\sigma = a_{i+1} \qquad \text{for } 1 \leqslant i < k; \qquad\qquad a_k\sigma = a_1;$$

and

$$x\sigma = x \qquad \text{for } x \notin \{a_1, a_2, \ldots, a_k\}.$$

*The **length** of such a cycle is k and we would refer to σ as a k**-cycle.** Note that the order of a k-cycle is k.*

Notation 59 ***Cycle notation:** We denote the above cycle as*

$$(a_1\, a_2\, a_3\, \cdots\, a_k).$$

Note that this notation isn't unique (in fact there are k such expressions in all) and that we have

$$(a_1\, a_2\, a_3\, \cdots\, a_k) = (a_2\, a_3\, a_4\, \cdots\, a_k\, a_1) = \cdots = (a_k\, a_1\, a_2\, \cdots\, a_{k-1}).$$

Example 60 *Note that α, β, γ, from Example 57 can be written as*

$$\alpha = (124), \qquad \beta = (13524), \qquad \gamma = (125)(34).$$

So α is a 3-cycle, β is a 5-cycle and γ is not a cycle.

Definition 61 *Two cycles* $(a_1 \dots a_k)$ *and* $(b_1 \dots b_l)$ *are said to be* ***disjoint*** *if* $a_i \neq b_j$ *for all* i, j.

Proposition 62 *Disjoint cycles commute.*

Proof. Let $\alpha = (a_1 \dots a_k)$ and $\beta = (b_1 \dots b_l)$. Then

$$\begin{array}{lll}
a_i\alpha\beta = a_{i+1}\beta = a_{i+1}, & a_i\beta\alpha = a_i\alpha = a_{i+1}, & \text{for } i < k; \\
a_k\alpha\beta = a_1\beta = a_1, & a_k\beta\alpha = a_k\alpha = a_1; & \\
b_i\alpha\beta = b_i\beta = b_{i+1}, & b_i\beta\alpha = b_{i+1}\alpha = b_{i+1}, & \text{for } i < l; \\
b_l\alpha\beta = b_l\beta = b_1, & b_l\beta\alpha = b_1\alpha = b_1; & \\
x\alpha\beta = x\beta = x, & x\beta\alpha = x\alpha = x, & \text{for } x \notin \{a_1, \dots, a_k, b_1, \dots, b_l\}.
\end{array}$$

■

Theorem 63 *Every permutation can be written as a product of disjoint cycles. This expression is unique up to the cycling of elements within cycles and permuting the order of the cycles.*

Proof. Let $\sigma \in S_n$ and let $a_1 \in \{1, 2, \dots, n\}$. Consider the sequence

$$a_1,\ a_1\sigma,\ a_1\sigma^2,\ a_1\sigma^3, \dots$$

As the elements of the sequence are in the set $\{1, 2, \dots n\}$ then the sequence must have repetitions so that $a_1\sigma^i = a_1\sigma^j$ for some $i < j$. But then $a_1\sigma^{j-i} = a_1$ is an earlier repetition of a_1 and we see that a_1 is in fact the first element of the sequence to repeat. Say $a_1\sigma^{k_1} = a_1$ is the first repetition of a_1. We see then that

$$\sigma \text{ acts on the set } \left\{a_1, a_1\sigma, a_1\sigma^2, \dots, a_1\sigma^{k_1-1}\right\} \text{ as the cycle } \left(a_1\, a_1\sigma\, a_1\sigma^2 \dots a_1\sigma^{k_1-1}\right).$$

The set $\left\{a_1, a_1\sigma, a_1\sigma^2, \dots, a_1\sigma^{k_1-1}\right\}$ is called the *orbit* of a_1.

If $k_1 = n$ then σ is a cycle and we are done. If not then we take a second element a_2 not in the orbit of a_1 and we can similarly see that σ acts as a second cycle on the orbit of a_2. These orbits are disjoint for if $a_1\sigma^i = a_2\sigma^j$ for some i, j then $a_2 = a_1\sigma^{i-j}$ and we see that a_2 was in the orbit of a_1, a contradiction. As the set $\{1, 2, \dots, n\}$ is finite then these orbits eventually exhaust the set and we see that

$$\sigma = \left(a_1\, a_1\sigma\, a_1\sigma^2 \dots a_1\sigma^{k_1-1}\right)\left(a_2\, a_2\sigma\, a_2\sigma^2 \dots a_2\sigma^{k_2-1}\right)\cdots\left(a_r\, a_r\sigma\, a_r\sigma^2 \dots a_1\sigma^{k_r-1}\right)$$

where r was the number of different orbits.

Suppose now that

$$\sigma = \rho_1\rho_2\cdots\rho_k = \tau_1\tau_2\cdots\tau_l$$

are expressions for σ as products of disjoint cycles. Then 1 appears in precisely one cycle ρ_i and in precisely one cycle τ_j. By reordering the appearances of the cycles if necessary (as they do commute, being disjoint) we may assume that 1 appears in ρ_1 and τ_1. By cycling the elements of the cycles ρ_1 and τ_1, if necessary, we may assume that 1 appears at the start of each cycle. Hence we see

$$\rho_1 = \left(1\, 1\sigma\, 1\sigma^2 \cdots 1\sigma^{k-1}\right) = \tau_1$$

where k is the size of the orbit of 1. By continuing similarly with an element not in the orbit of 1 we can show (with permitted permuting of cycles and cycling within cycles) that $\rho_2 = \tau_2$ etc. to complete the proof. ■

Definition 64 *As a consequence of the above theorem, the lengths of the various cycles of a permutation and the number of cycles of each such length, is well-defined. The is known as the* ***cycle decomposition type*** *(or just* ***cycle type****) of the permutation.*

Example 65 *Write the following permutations in S_9 as products of disjoint cycles.*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 9 & 7 & 3 & 2 & 4 & 8 & 1 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 7 & 5 & 1 & 3 & 6 & 2 & 8 \end{pmatrix}.$$

Write α^{-1} and β^{272} as products of disjoint cycles.

Solution. We see that

$$1 \xrightarrow{\alpha} 5 \xrightarrow{\alpha} 3 \xrightarrow{\alpha} 9 \xrightarrow{\alpha} 1, \qquad 2 \xrightarrow{\alpha} 6 \xrightarrow{\alpha} 2, \qquad 4 \xrightarrow{\alpha} 7 \xrightarrow{\alpha} 4, \qquad 8 \xrightarrow{\alpha} 8$$

and so

$$\alpha = (1539)\,(26)\,(47)\,(8)\,.$$

Hence we also see

$$\alpha^{-1} = (1935)\,(26)\,(47)\,(8)\,.$$

We also see

$$1 \xrightarrow{\beta} 4 \xrightarrow{\beta} 5 \xrightarrow{\beta} 1, \qquad 2 \xrightarrow{\beta} 9 \xrightarrow{\beta} 8 \xrightarrow{\beta} 2, \qquad 3 \xrightarrow{\beta} 7 \xrightarrow{\beta} 6 \xrightarrow{\beta} 3,$$

so that

$$\beta = (145)\,(298)\,(376)\,.$$

We then see that

$$\beta^k = (145)^k\,(298)^k\,(376)^k = \begin{cases} e & k \text{ is a multiple of 3;} \\ \beta & k-1 \text{ is a multiple of 3;} \\ \beta^2 & k-2 \text{ is a multiple of 3.} \end{cases}$$

as disjoint cycles commute. Hence

$$\beta^{272} = \beta^2 = (154)\,(289)\,(367)\,.$$

■

Notation 66 ***Suppressing 1-cycles.*** *It is typical to not bother writing 1-cycles (or fixed points) of permutations. So – for α, α^{-1} as in the previous example – we will write*

$$\alpha = (1539)\,(26)\,(47) \qquad \textit{and} \qquad \alpha^{-1} = (1935)\,(26)\,(47)$$

with it being understood that 8 is not moved (or more generally any unmentioned elements).

Proposition 67 *Let $\sigma = \rho_1 \cdots \rho_k$ be an expression for σ as disjoint cycles of lengths $l_1, \ldots, l_k$. Then the order of σ equals*

$$\mathrm{lcm}(l_1, \ldots l_k)$$

where lcm *denotes the lowest common multiple. (Given finitely many positive integers, their* ***least common multiple*** *is the smallest positive integer which is a multiple of each of them.)*

Example 68 *(i) How many* 5*-cycles are there in* S_{11}*?*
(ii) How many permutations in S_8 *have a cycle decomposition type of two* 3*-cycles and one* 2*-cycle?*

Solution. (i) 5-cycles in S_{11} are of the form $(a\,b\,c\,d\,e)$. There are 11 choices for what a might be, 10 for b, 9 for c, 8 for d and 7 for e. However we need to remember that

$$(a\,b\,c\,d\,e) = (b\,c\,d\,e\,a) = (c\,d\,e\,a\,b) = (d\,e\,a\,b\,c) = (e\,a\,b\,c\,d)$$

and so there answer is

$$\frac{11 \times 10 \times 9 \times 8 \times 7}{5} = 11088.$$

(ii) Permutations in S_8 that decompose to two 3-cycles and a 2-cycles are of the form

$$(a\,b\,c)\,(d\,e\,f)\,(g\,h)\,.$$

There are 8! ways of filling in these brackets as $a \ldots h$ but we need to remember that the above permutation also equals

$$(b\,c\,a)\,(d\,e\,f)\,(g\,h) = (a\,b\,c)\,(e\,f\,g)\,(g\,h) = (a\,b\,c)\,(d\,e\,f)\,(h\,g) = (d\,e\,f)\,(a\,b\,c)\,(g\,h)\,.$$

The first three are equivalent rewritings that come from cycling elements within cycles whilst the last one comes from permuting two equal length cycles. Hence the number of such permutations is

$$\frac{8!}{3 \times 3 \times 2! \times 2} = \frac{40320}{36} = 1120.$$

(i') Note that we could have tackled the 5-cycle question in this manner as well. Thinking of 5-cycles in S_{11} as having cycle type

$$(a\,b\,c\,d\,e)\,(f)\,(g)\,(h)\,(i)\,(j)\,(k)$$

we see that there are 11! ways of filling these brackets as $a \ldots k$ but 5 ways of cycling $a \ldots e$ and 6! ways of permuting the equal length cycles $(f) \ldots (k)$ Hence the answer is

$$\frac{11!}{5 \times 6!} = 11088.$$

■

Proposition 69 *In* S_n *there are*

$$\frac{n!}{\left(l_1^{k_1} \times l_2^{k_2} \times \cdots \times l_r^{k_r}\right)\left(k_1! \times k_2! \times \cdots \times k_r!\right)}$$

permutations with a cycle type of k_1 *cycles of length* l_1*,* k_2 *cycles of length* $l_2, \ldots, k_r$ *cycles of length* l_r*. This decomposition includes* 1*-cycles so that*

$$k_1 l_1 + k_2 l_2 + \cdots + k_r l_r = n.$$

Proof. Put in a fixed order the $\sum k_i$ brackets. As already argued in specific cases, there are $n!$ ways of filling the brackets with the numbers $1, \ldots, n$. However the same permutation can be written as a product of disjoint cycles in many ways as specified in Theorem 63 (though essentially these all being the same). From that theorem we know that there are l_i ways of cycling the elements of each cycle of length l_i and we have $k_i!$ of permuting the cycles of length l_i. Hence $n!$ is an overcount by a factor of

$$\left(l_1^{k_1} \times l_2^{k_2} \times \cdots \times l_r^{k_r}\right)\left(k_1! \times k_2! \times \cdots \times k_r!\right).$$

■

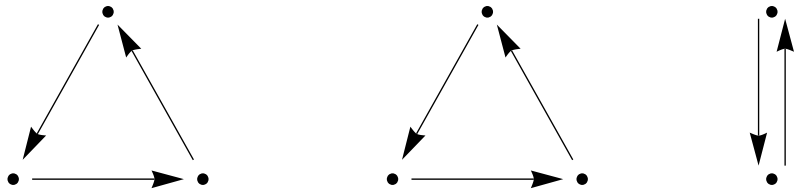
Example 70 *How many permutations of each cycle type are there in S_7?*

Solution. The table below contains the various numbers. We need to consider the various ways in which 7 can be composed as other integers.

type	working	#	type	working	#	type	working	#
7	$7!/7$	720	$4+2$	$7!/(4\times 2)$	630	3	$\frac{7\times 6\times 5}{3}$	70
6	$7!/6$	840	4	$\frac{7\times 6\times 5\times 4}{4}$	210	3×2	$\frac{7\times 6\times 5\times 4\times 3\times 2}{2\times 2\times 2\times 3!}$	105
$5+2$	$7!/(5\times 2)$	504	2×3	$\frac{7\times 6\times 5\times 4\times 3\times 2}{3\times 3\times 2!}$	280	2×2	$\frac{7\times 6\times 5\times 4}{2\times 2\times 2!}$	105
5	$\frac{7\times 6\times 5\times 4\times 3}{5}$	504	$3+2\times 2$	$\frac{7!}{3\times 2\times 2\times 2!}$	210	2	$\frac{7\times 6}{2}$	21
$4+3$	$7!/(4\times 3)$	420	$3+2$	$\frac{7\times 6\times 5\times 4\times 3}{3\times 2}$	420	e		1

■

Without the labels $1, 2, \ldots, n$ two permutations of the same cycle type would be indistinguishable. For example, a permutation in S_8 which consists of two 3-cycles and one 2-cycle would simply look like



if we were ignorant of which of the eight objects were $1, 2, \ldots, 8$. Here each arrow represents the effect of applying the permutation once. This idea can be more formally captured by the idea of *conjugates*.

Definition 71 *Two permutations $\sigma, \tau \in S_n$ are said to be **conjugate** in S_n if there exists $\rho \in S_n$ such that*

$$\sigma = \rho^{-1}\tau\rho.$$

Theorem 72 *Two permutations $\sigma, \tau \in S_n$ are conjugate if and only if they have the same cycle type. (i.e. for any given length, the two permutations have the same number of cycles of that length.)*

We first note the following:

Lemma 73 *For any cycle* $(a_1\, a_2\, \ldots\, a_k)$ *and any* $\rho \in S_n$ *we have*

$$\rho^{-1}(a_1\, a_2\, \ldots\, a_k)\rho = (a_1\rho\, a_2\rho\, \ldots\, a_k\rho).$$

Proof. (Of Lemma) This is left to Exercise Sheet 2, Question 3. ■

Proof. (Of Theorem.) Suppose that $\tau = \rho^{-1}\sigma\rho$ and that $\sigma = \psi_1\psi_2 \ldots \psi_r$ where the ψ_i are disjoint cycles. Then

$$\tau = \rho^{-1}\left(\psi_1\psi_2 \ldots \psi_r\right)\rho = \left(\rho^{-1}\psi_1\rho\right)\left(\rho^{-1}\psi_2\rho\right)\cdots\left(\rho^{-1}\psi_r\rho\right)$$

and we see by the previous lemma that the $\rho^{-1}\psi_i\rho$ are disjoint cycles of the same lengths as the ψ_i. Conversely, suppose that σ and τ have the same cycle decomposition type. Then we may line up the cycles in σ and τ of corresponding lengths as

$$\begin{array}{ccccccc} \sigma & = & (a_1\, a_2\, \ldots\, a_k) & (b_1\, b_2\, \ldots\, b_l) & (c_1\, c_2\, \ldots\, c_m) & \cdots \\ & & \downarrow \rho & \downarrow \rho & \downarrow \rho & \downarrow \rho \\ \tau & = & (\alpha_1\, \alpha_2\, \ldots\, \alpha_k) & (\beta_1\, \beta_2\, \ldots\, \beta_l) & (\gamma_1\, \gamma_2\, \ldots\, \gamma_m) & \cdots \end{array}$$

and we define ρ by $a_i\rho = \alpha_i$, $b_i\rho = \beta_i$, $c_i\rho = \gamma_i$, etc. We then have

$$\begin{array}{rcl} \alpha_i\left(\rho^{-1}\sigma\rho\right) & = & a_i\sigma\rho = a_{i+1}\rho = \alpha_{i+1} = \alpha_i\tau \quad \text{for} \quad 1 \leqslant i < k \\ \alpha_k\left(\rho^{-1}\sigma\rho\right) & = & a_k\sigma\rho = a_1\rho = \alpha_1 = \alpha_k\tau \end{array}$$

and similarly for the other cycles. ■

Example 74 *Let*

$$\sigma = (12)\,(34)\,(567)\,, \qquad \tau = (28)\,(17)\,(345)$$

be permutations in S_8.

(i) How many ρ *are there in* S_8 *such that* $\sigma = \rho^{-1}\tau\rho$*?*

(ii) How many $\rho \in S_8$ *are there which commutes with* σ*?*

Solution. (i) We need ρ such that

$$\rho^{-1}\tau\rho = (2\rho\, 8\rho)\,(1\rho\, 7\rho)\,(3\rho\, 4\rho\, 5\rho) = (12)\,(34)\,(567)\,.$$

Thinking about the different ways of rewriting $(12)\,(34)\,(567)$ (as the same permutation) we see that we need

$$(2\rho\, 8\rho)\,(1\rho\, 7\rho) = (12)\,(34) \quad \text{and} \quad (3\rho\, 4\rho\, 5\rho) = (567)\,.$$

and so

$$3\rho = 5 \text{ or } 6 \text{ or } 7, \qquad 2\rho = 1 \text{ or } 2 \text{ or } 3 \text{ or } 4, \qquad 6\rho = 8.$$

Once we know 3ρ then 4ρ and 5ρ are known (e.g. $3\rho = 6$ implies $4\rho = 7$ and $5\rho = 5$). Once we know 2ρ then we know 8ρ but we still have two choices for 1ρ. In all then we see that there are

$$\underbrace{3}_{\text{choosing } 3\rho} \times \underbrace{4}_{\text{choosing } 2\rho} \times \underbrace{2}_{\text{choosing } 1\rho} = 24$$

such ρ.

(ii) If we replace τ with σ we can still make the same argument to realize that there are 24 such ρ that $\sigma = \rho^{-1}\sigma\rho$. However this is an equivalent equation to $\rho\sigma = \sigma\rho$ so these same 24 permutations commute with σ. ■

Remark 75 *If further asked which these* 24 *permutations are recall that we need*

$$(1\rho\, 2\rho)\,(3\rho\, 4\rho)\,(5\rho\, 6\rho\, 7\rho) = (12)\,(34)\,(567)\,.$$

So the 24 *permutations in fact comprise the group* $D_8 \times C_3$ *where* D_8 *is the symmetry group of the square with labels* $1, 2$ *on one diagonal and* $3, 4$ *on another and* $C_3 = \{e, (567), (576)\}$.

Recall now the definition of a *permutation matrix* from Linear Algebra II:

Definition 76 *(i) An* $n \times n$ *matrix is a* ***permutation matrix*** *if each row and each column contain a single entry* 1 *and all other entries are* 0.

(ii) We can associate with $\sigma \in S_n$ *a permutation matrix* P_σ *such that the* 1 *entry in row* i *of* P_σ *is in column* $i\sigma$.

Note that the (i, j)*th entry of* P_σ *is* $\delta_{i\sigma\, j}$.

Example 77 *With* $n = 3$:

$$P_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad P_{(123)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \qquad P_{(132)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Note that $P_{(12)}$ *is self-inverse and that* $P_{(123)}$ *is the inverse of* $P_{(132)}$.

Proposition 78 *(a) For* $\sigma \in S_n$ *then* P_σ *is indeed a permutation matrix.*

(b) For $\sigma, \tau \in S_n$ *then* $P_{\sigma\tau} = P_\sigma P_\tau$.

Proof. (a) By definition P_σ has precisely a single entry 1 in each row. And the only row with an entry of 1 in the ith column is row $i\sigma^{-1}$.

(b) By definition of matrix multiplication

$$(P_\sigma P_\tau)_{ij} = \sum_{k=1}^{n} (P_\sigma)_{ik}\,(P_\tau)_{kj} = \sum_{k=1}^{n} \delta_{i\sigma\, k}\,\delta_{k\tau\, j} = \delta_{i\sigma\tau\, j} = (P_{\sigma\tau})_{ij}\,.$$

■

We will make use of permutation matrices in showing that the *parity* of a permutation is well-defined.

Definition 79 *(i) A* ***transposition*** *is another term for a* 2*-cycle.*

(ii) A permutation is said to be ***odd*** *(resp.* ***even****) if it can be written as a product of an odd (resp. even) number of transpositions.*

Lemma 80 *If* σ *is a transposition then* $\det P_\sigma = -1$.

Proof. This is equivalent to knowing that swapping two rows of a matrix multiplies its determinant by -1. For if $\sigma = (ij)$ then

$$\det P_\sigma = \det\left(I_n \text{ with rows } i \text{ and } j \text{ swapped}\right) = -\det I_n = 1.$$

■

Theorem 81 *(a) Every permutation can be written as a product of transpositions (and consequently is either even and/or odd).*

(b) No permutation is both even and odd.

Proof. (a) Any permutation my be written as a product of disjoint cycles by Theorem 63. And any cycle may be written as a product of transpositions as

$$(a_1\, a_2\, a_3 \cdots a_k) = (a_1 a_2)\,(a_1 a_3) \cdots (a_1 a_k)$$

as the product of transpositions has the effect

$$a_1 \underbrace{\rightarrow}_{(a_1 a_2)} a_2 \underbrace{\rightarrow}_{\text{remainder}} a_2, \qquad a_i \underbrace{\rightarrow}_{\text{first } i-2} a_i \underbrace{\rightarrow}_{(a_1 a_i)} a_1 \underbrace{\rightarrow}_{(a_1 a_{i+1})} a_{i+1} \underbrace{\rightarrow}_{\text{remainder}} a_{i+1} \quad \text{for } i \geqslant 2.$$

(b) If σ is expressible as the product of k transpositions, then by the above lemma $\det P_\sigma = (-1)^k$. Hence no permutation can be both even and odd. ■

Remark 82 *Note that cycles of even (resp. odd) length are (somewhat annoyingly) odd (resp. even). So a permutation is even if and only if its cyclic type has an even number of even length cycles.*

Example 83 *If we return to Example 70 then we see that the following permutations were the even ones.*

type	*working*	#	*type*	*working*	#	*type*	*working*	#
7	$7!/7$	720	2×3	$\frac{7\times6\times5\times4\times3\times2}{3\times3\times2!}$	280	2×2	$\frac{7\times6\times5\times4}{2\times2\times2!}$	105
5	$\frac{7\times6\times5\times4\times3}{5}$	504	$3 + 2 \times 2$	$\frac{7!}{3\times2\times2\times2!}$	210	e		1
$4 + 2$	$7!/(4 \times 2)$	630	3	$\frac{7\times6\times5}{3}$	70		*TOTAL*	2520

Note that precisely half the permutations are even.

Proposition 84 *(a) The even permutations in S_n form a subgroup A_n.*
(b) For $n \geqslant 2$, the order of A_n is $\frac{1}{2}n!$.
(c) A_n is non-abelian for $n \geqslant 4$.
*A_n is called the **alternating group**.*

Proof. (a) If

$$\sigma = \rho_1\rho_2 \cdots \rho_{2k} \qquad \text{and} \qquad \tau = \psi_1\psi_2 \cdots \psi_{2l}$$

are expressions for σ and τ as products of even numbers of transpositions then

$$\sigma\tau = \rho_1\rho_2 \cdots \rho_{2k}\psi_1\psi_2 \cdots \psi_{2l} \qquad \text{and} \qquad \sigma^{-1} = \rho_{2k}\rho_{2k-1} \cdots \rho_1$$

are clearly even. The identity is also even as e is the product of zero transpositions. Hence A_n is a subgroup of S_n.

(b) The permutation (12) is odd; so the maps

$$A_n \to A_n^c \text{ given by } \sigma \mapsto (12)\sigma; \qquad A_n^c \to A_n \text{ given by } \sigma \mapsto (12)\sigma;$$

are inverses of one another and so $|A_n| = |A_n^c| = \frac{1}{2}n!$.

(c) If $n \geqslant 4$ then note (123) and (124) are even permutations which do not commute. ■

Example 85 (123) *and* (132) *are not conjugate in* A_4.

Solution. Suppose that $\sigma^{-1}(123)\sigma = (132)$. Then $(1\sigma\, 2\sigma\, 3\sigma) = (132)$. As

$$(132) = (213) = (321)$$

are the only ways to write the permutation (132) then there are three possibilities

$$\begin{array}{rcl} 1\sigma & = & 1, \quad 2\sigma = 3, \quad 3\sigma = 2, \quad 4\sigma = 4; \\ 1\sigma & = & 2, \quad 2\sigma = 1, \quad 3\sigma = 3, \quad 4\sigma = 4; \\ 1\sigma & = & 3, \quad 2\sigma = 2, \quad 3\sigma = 1, \quad 4\sigma = 4. \end{array}$$

That is σ equals (23) or (12) or (13). As none of these is even, then (123) and (132) are not conjugate in A_4. ■

Example 86 *The conjugacy classes in* A_4 *are* $\{e\}$ *and*

$$\{(12)(34),(13)(24),(14)(23)\}, \quad \{(123),(134),(214),(324)\}, \quad \{(132),(143),(124),(234)\}.$$

Solution. Note that

$$(123)^{-1}(12)(34)(123) = (23)(14), \qquad (123)^{-1}(23)(14)(123) = (31)(24).$$

Also

$$(123)^{-1}(134)(123) = (214), \quad (123)^{-1}(214)(123) = (324), \quad (134)^{-1}(214)(134) = (123).$$

As conjugacy in A_4 implies conjugacy in S_4 (though not conversely) and a 3-cycle is not conjugate in A_4 with its inverse (by the previous example), then the conjugacy classes in A_4 are as given. ■